

CYBERSECURITY

Coordinated Vulnerability Disclosure Policy

KRÜSS setzt sich für die Sicherheit seiner Produkte, Software, Dienste und IT-Infrastruktur ein. Für Meldungen zu möglichen Cybersicherheits-Schwachstellen nutzen wir einen Prozess zur Coordinated Vulnerability Disclosure. Dieser orientiert sich am Cyber Resilience Act, an BSI TR-03183-3 sowie an EN ISO/IEC 29147 und EN ISO/IEC 30111.

Wir nehmen Meldungen zu KRÜSS Produkten mit digitalen Elementen, zugehöriger Firmware und Software, offiziellen Web- und Cloud-Diensten sowie unserer IT-Infrastruktur entgegen. Meldungen sind unabhängig von Servicevertrag und Produktlebenszyklus willkommen.

Zusammenarbeit in gutem Glauben

Wir behandeln Meldungen und personenbezogene Daten im gesetzlich zulässigen Umfang vertraulich. Für eine Meldung verlangen wir keine Geheimhaltungsvereinbarung. KRÜSS wird keine eigenen rechtlichen Schritte gegen Personen einleiten, die in gutem Glauben handeln und diese Policy einhalten, insbesondere indem sie:

- nur eigene oder ausdrücklich freigegebene Produkte und Systeme prüfen und dabei keine Kunden beeinträchtigen;
- geltendes Recht einhalten und Sicherheit, Privatsphäre, Messdaten, Audit Trails sowie Labor- und Produktionsabläufe schützen;
- keine Social-Engineering-, Brute-Force-, Denial-of-Service-, Last- oder destruktiven Tests durchführen;
- die Prüfung einer möglichen Schwachstelle auf den für ihren Nachweis erforderlichen Umfang beschränken. Eigene Daten oder ausdrücklich für die Prüfung freigegebene Daten dürfen dabei verändert oder gelöscht werden, soweit dies für den Nachweis erforderlich ist;
- die Prüfung bei unbeabsichtigtem Zugriff auf andere Daten sofort beenden. Diese Daten dürfen nicht verändert, gelöscht, verwendet oder weitergegeben werden;
- dabei erlangte personenbezogene, vertrauliche oder nicht öffentliche Informationen löschen und weder verwenden noch an Dritte weitergeben;
- technische Einzelheiten erst nach dem abgestimmten Offenlegungszeitpunkt veröffentlichen.

Diese Zusage gilt nicht bei erkennbar krimineller Absicht, vorsätzlicher Schädigung, Erpressung oder erheblicher Missachtung dieser Regeln. Sie bindet keine Dritten und erteilt keine Genehmigung zum Zugriff auf fremde Systeme oder Daten.

Ablauf

Meldung

Senden Sie die Meldung möglichst verschlüsselt an security@kruss. Bei erreichbarbarem Rückkanal bestätigen wir den Eingang innerhalb von fünf Arbeitstagen. Beschreiben Sie bitte beobachtetes und erwartetes Verhalten, Auswirkung, betroffenes Produkt oder System (möglichst mit Modell, Seriennummer und Version) sowie reproduzierbare Schritte oder einen Proof of Concept. Ergebnisse automatisierter Scans benötigen nachvollziehbare Belege. Teilen Sie uns außerdem mit, ob die Schwachstelle bereits öffentlich bekannt ist oder aktiv ausgenutzt wird.

Analyse

Wir prüfen und reproduzieren die gemeldete Schwachstelle und stellen bei Bedarf Rückfragen. Bei erreichbarbarem Rückkanal erhalten Sie innerhalb von zehn Arbeitstagen eine qualifizierte Rückmeldung oder eine Information, warum die Prüfung länger dauert und wann das nächste Update erfolgt.

Behebung

Bestätigte Schwachstellen bearbeiten wir mit den zuständigen Entwicklungs-, Service- und IT-Teams. Der Lebenszyklusstatus des betroffenen Produkts kann die mögliche Abhilfe beeinflussen. Währenddessen halten wir Kontakt mit der meldenden Person, sofern ein Rückkanal verfügbar ist.

Veröffentlichung

Bestätigte Schwachstellen bearbeiten wir risikobasiert. Sobald ein Security Update, ein Workaround oder eine andere geeignete Abhilfemaßnahme verfügbar ist, veröffentlicht KRÜSS die erforderlichen Informationen in einem Security Advisory auf der KRÜSS Website. Das Advisory enthält insbesondere Angaben zu den betroffenen Produkten und Versionen, den Auswirkungen und dem Schweregrad sowie zu verfügbaren Updates oder anderen Abhilfemaßnahmen. In begründeten Fällen kann die Veröffentlichung zurückgestellt werden, bis betroffene Nutzer eine angemessene Möglichkeit hatten, die Abhilfemaßnahme umzusetzen. Gesetzliche Meldepflichten gegenüber den zuständigen Stellen bleiben unberührt.

KRÜSS kann meldende Personen mit deren Zustimmung namentlich oder unter einem Alias würdigen. Ein Anspruch auf Vergütung oder Kostenerstattung besteht nicht; KRÜSS betreibt kein Bug-Bounty-Programm.

Kontakt

E-Mail	security@kruss.de
OpenPGP-Schlüssel	kruss-scientific.com/.well-known/security-key.asc
security.txt	kruss-scientific.com/.well-known/security.txt
Sprachen	Deutsch und Englisch

Weitere Informationen zum Datenschutz

kruss-scientific.com/de-DE/datenschutzerklaerung

CYBERSECURITY

Coordinated Vulnerability Disclosure Policy

KRÜSS is committed to the security of its products, software, services, and IT infrastructure. We use a Coordinated Vulnerability Disclosure process for reports of potential cybersecurity vulnerabilities. The process is guided by the Cyber Resilience Act, BSI TR-03183-3, EN ISO/IEC 29147, and EN ISO/IEC 30111.

We accept reports concerning KRÜSS products with digital elements, related firmware and software, official web and cloud services, and our IT infrastructure. Reports are welcome regardless of service contract or product lifecycle.

Good Faith Cooperation

We treat reports and personal data as confidential to the extent permitted by law. We do not require a non-disclosure agreement for submission. KRÜSS will not initiate legal action against individuals who act in good faith and comply with this policy, in particular by:

- testing only their own or expressly authorized products and systems without affecting customers;
- complying with applicable law and protect safety, privacy, measurement data, audit trails, and laboratory and production operations;
- not conducting social engineering, brute-force, denial-of-service, load or destructive testing;
- limiting testing of a potential vulnerability to the extent necessary to demonstrate it. Their own data or data expressly authorized for testing may be modified or deleted where necessary to demonstrate the vulnerability;
- stopping testing immediately upon unintended access to other data. Such data must not be modified, deleted, used or disclosed;
- deleting any personal, confidential, or non-public information obtained in the process and neither using it nor disclosing it to third parties;
- publishing technical details only after the coordinated disclosure date.

This assurance does not apply in cases of apparent criminal intent, deliberate harm, extortion, or another material breach of these rules. It does not bind third parties or authorize access to third-party systems or data.

Process

Reporting

Send the report, preferably encrypted, to security@kruss.de. Where a return channel is available, we acknowledge receipt within five working days. Please describe the observed and expected behavior, impact, affected product or system (including model, serial number, and version where available), and reproducible steps or a proof of concept. Automated scan results require supporting evidence. Also tell us whether the vulnerability is already public or is being actively exploited

Analysis

We investigate and reproduce the reported vulnerability and request further information where needed. Where a return channel is available, we provide substantive feedback within ten working days or explain why the investigation needs more time and when the next update will be provided.

Resolution

We address confirmed vulnerabilities with the responsible development, service, and IT teams. The lifecycle status of the affected product may influence the available remediation. During this period, we remain in contact with the reporter where a return channel is available.

Disclosure

We address confirmed vulnerabilities based on risk. Once a security update, workaround or other appropriate remediation is available, KRÜSS publishes the necessary information in a security advisory on the KRÜSS website. The advisory includes, in particular, information on affected products and versions, impact and severity, and available updates or other remediation measures. In justified cases, publication may be deferred until affected users have had a reasonable opportunity to implement the remediation. Statutory reporting obligations to the competent authorities remain unaffected.

With the reporter's consent, KRÜSS may provide acknowledgement by name or alias. There is no entitlement to payment or reimbursement of costs; KRÜSS does not operate a bug bounty program.

Contact

Email	security@kruss.de
OpenPGP key	kruss-scientific.com/.well-known/security-key.asc
security.txt	kruss-scientific.com/.well-known/security.txt
Languages	German and English

Further information on data protection

kruss-scientific.com/en/data-privacy-statement